



DEFENSE INTELLIGENCE AGENCY
Chief, Planning Division,
Directorate for Management
and Plans (DP-1)

DP

8/11

For you to
bring with you
when going to
[redacted] (DS
Treaty on Leaks)

Rockefeller
Church } common with

good
probe

AP

←

DIA review Completed.

05000000



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE (INTELLIGENCE)/
DIRECTOR OF DEFENSE INTELLIGENCE

WASHINGTON, D. C. 20301

MEMORANDUM FOR THE SPECIAL ASSISTANT TO THE DEPUTY TO THE DCI FOR THE
INTELLIGENCE COMMUNITY

SUBJECT: Impact of Leaks on the Conduct of Intelligence (U)

Reference: My memorandum to you of 29 July 1976, same subject.

(U) This memorandum provides additional comments concerning damage caused to our foreign intelligence collection programs by unauthorized disclosures of sensitive intelligence information.

(U) Our experience indicates this is a "people" rather than a "system" problem. There would be no unauthorized disclosures or security violations if the regulations prescribing information security procedures were followed. Additionally, there are security procedures for expeditious review for public disclosure of classified information.

(C) We have observed that the more damaging intelligence disclosures result primarily from unauthorized disclosures made to representatives of the news media. The timing and nature of unauthorized disclosures of sensitive intelligence information indicate that most are being made in the Greater Washington area by personnel interested in supporting a particular cause or policy. Not all of these leaks originate in the Executive Branch of the Government. Investigations of unauthorized disclosures of sensitive intelligence to representatives of the news media have been conducted primarily to attempt to identify the "leaker." In some instances, we have been prone to accept assessments indicating grave damage to sensitive sources and methods when, in fact, the compromised information was from, rather than about, the source and/or method concerned.

(U) The agencies in the Intelligence Community which produce intelligence reports have repeatedly reviewed the dissemination of such reports in order to reduce the volume disseminated if possible. In spite of such efforts, there is still a relatively wide and necessary dissemination of reports which, together with investigative limitations, make it difficult, if not impossible, to identify the person(s) making unauthorized disclosures.

Classified by DIARCI
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY 2
DECLASSIFY ON upon notification of
originator

SECRET

NOT RELEASABLE TO FOREIGN NATIONALS



SECRET

(C) All so-called press "leaks" do not necessarily result from unauthorized disclosures. In some instances, chance or inadvertent disclosures provide clues that capable aggressive investigative reporters can pursue. Combining such information with other bits and pieces, utilizing such excellent sources of information as Congressional testimony, and performing what amounts to intelligence analysis, these reporters may well prepare articles containing information the Government maintains as highly classified. When unsuccessful in satisfying their story requirements through normal public affairs channels, the news media representatives many times develop their own sources. Frequently officials in the Washington area, particularly those newly assigned, are at a loss as to how to react to aggressive reporters when direct contacts are made. They are unaware as to what extent policy permits or encourages their cooperation with the news media. Officials who are called on to brief reporters are in a particularly vulnerable position when the subject being briefed has many aspects that are classified.

(U) The assignment of TOP SECRET, SECRET, or CONFIDENTIAL markings should provide adequate protection to the overwhelming majority of intelligence reports. The placing of unwarranted restrictive handling caveats on such reports degrades the entire information security system. Many recipients of intelligence information, however, are unsure as to what specific information is classified. The classification guide is an essential part of the security program. Vast sums of money are expended in safeguarding classified information and great detail given to controlling and accounting for classified documents. But not enough attention seems to be given to the actual act of classifying information. When some official classifies information, this causes such information to be entered into a system of guards, safes, locks, alarms, vaults, security investigations, controls and accountability -- not to mention the very complex and expensive industrial security program to protect the production of classified hardware. Quite often classification actions are subjective and without any substantial basis for classification in the first place. Up-to-date classification guides, in proper content and in a usable format, covering all plans, programs and projects will provide for consistent and justifiable classification actions.

(S/NOFORN) Establishing a direct correlation between an unauthorized disclosure and an intelligence loss is not easy. In some cases, the loss may not become evident for some time. In other cases, the sensitive source may be prejudiced but not compromised to the point of rendering them ineffective. For example:

SECRET**NOT RELEASABLE TO FOREIGN NATIONALS**

Page Denied

requiring the use of bona fide intelligence as "feed" material. Still another possible area of concern involves the release of sensitive intelligence information to friendly countries. These countries normally do not report possible compromises and the results of possible hostile intelligence operations unless such information is first disclosed in the public realm. Our sanitization efforts prior to release of intelligence to such nations are designed to protect sensitive intelligence sources and methods.

(C) The following actions are being taken to cope with the problem of unauthorized disclosures of sensitive and highly classified intelligence information:

a. A permanent Working Group of the Director of Central Intelligence Security Committee (SECOM) has been established to address the problem of unauthorized disclosures. This Working Group, chaired by the DIA alternate member of the SECOM, will take actions to insure the timely and coordinated investigation of unauthorized disclosures of intelligence information by the affected member agencies or departments of the Intelligence Community. Reports will be made by the Chairman, SECOM to the DCI as required and will include the degree of damage, if any, to sensitive intelligence collection sources and methods. The SECOM will also be the central office of record for the Intelligence Community for these unauthorized disclosures.

b. General Wilson has initiated a study, in coordination with the J-5, OJCS to identify, if possible, the extent to which unauthorized disclosures of sensitive intelligence information has caused, or is causing, our military planners to make changes in the U.S. force structure; training doctrine; and in equipment programmed for the Armed Forces.

c. DepSecDef Ellsworth has proposed the establishment of a Public Advisory Committee on the Security and Disclosure of Information. This Committee will address itself to the problem of securing better protection for those secrets, including not only intelligence data and methods, but military and diplomatic secrets as well, to the extent that their protection is the responsibility of the Department of Defense. Attempts by foreign powers or their agents to obtain government secrets will not be addressed by the Committee.

(U) It is concluded that:

a. Highly sensitive intelligence information can be protected over extended periods of time only by severely limiting access to such information.

~~SECRET~~

b. While measures must be taken to reduce the number of "leaks," it will be difficult to completely eliminate such unauthorized disclosures because of the nature of our open society, with its aggressive and competent investigative reporters and special interest groups.

c. Additional effort be made to insure that finished intelligence receiving general dissemination does not contain sensitive information about the source.

~~Thomas K. Latimer
Principal Deputy~~

*Not
Signed*

History note re SECOM

*History
note
"General
can
IC staff"*

*good point -
don't
include
source info
in
"pushed
info"*

~~SECRET~~